WHAT IS CLAIMED IS:

1. A device for processing an image, the device comprising:

a decryption module configured to receive graphics data, wherein at least a portion of the received graphics data is encrypted, and to decrypt the graphics data based at least in part on a decryption parameter;

a key module configured to receive key data and to provide the decryption parameter to the decryption module in response to the key data; and

an image generation module coupled to receive the decrypted graphics data from the decryption module and configured to transform the decrypted graphics data to displayable image data.

2. The device of claim 1 wherein the decryption module is further configured to provide the encrypted graphics data to the image generation module in the event that the key module does not provide the decryption parameter.

3. The device of claim 1 wherein the encrypted portion of the graphics data is encrypted by applying a perturbation, the perturbation being removable by the decryption module.

4. The device of claim 1 wherein the key data includes the decryption parameter.

5. The device of claim 1 wherein the key module is further configured to compute the decryption parameter using the key data.

6. The device of claim 1 wherein the key module includes a receptacle for a key device and wherein the key module is further configured to obtain the key data from the key device.

7. The device of claim 6 wherein the decryption parameter corresponds to the presence or absence of the key device in the receptacle.

8. The device of claim 6 wherein the key device is configured to store the key data and the key module is configured to read the key data when the key device is present in the receptacle.

9. The device of claim 1 wherein the key module receives the key data from a sender and the decryption module receives the graphics data from the same sender.

10. The device of claim 1 wherein the key module is further configured to receive either of first key data and second key data and to provide a first decryption parameter in response to the first key data and a second decryption parameter in response to the second key data,

wherein in response to the first decryption parameter, the decryption module completely decrypts the graphics data and, in response to the second decryption parameter, the decryption module decrypts the graphics data with a residual distortion.

11. A system for generating images, the system comprising:

a sender device configured to send graphics data via a communication channel, wherein at least a portion of the graphics data is encrypted;

a recipient device including:

a decryption module configured to receive the encrypted graphics data and to decrypt the graphics data based at least in part on a decryption parameter;

a key module configured to receive key data and to provide the decryption parameter to the decryption module in response to the key data; and

an image generation module coupled to receive the decrypted graphics data from the decryption module and configured to transform the graphics data to displayable image data.

12. The system of claim 11 wherein the sender device and the recipient device communicate via a bus.

13. The system of claim 12 wherein the sender device is a central processing unit and the recipient device includes a graphics processing unit.

14. The system of claim 11 wherein the sender device and the recipient device communicate via a network.

15. The system of claim 11 wherein the key module includes a receptacle for a key device, the key device providing the key data to the key module.

16. The system of claim 11 wherein the key data includes the decryption parameter.

17. The system of claim 11 wherein the key module is further configured to compute the decryption parameter using the received key data.

18. The system of claim 11 wherein the key module is configured to receive either of first key data and second key data and further configured to provide a first decryption parameter in response to the first key data and a second decryption parameter in response to the second key data,

wherein in response to the first decryption parameter, the decryption module completely decrypts the graphics data and, in response to the second decryption parameter, the decryption module decrypts the graphics data with a residual distortion.

19. A method of generating an image, the method comprising:

receiving graphics data for the image, wherein at least a portion of the received graphics data is encrypted;

determining whether a key is present; and

in response to determining that the key is present:

decrypting the encrypted portion of the graphics data; and

rendering an image using the decrypted graphics data.

20. The method of claim 19, further comprising:

in response to determining that the key is not present, rendering an image using the received graphics data including the encrypted portion.

21. The method of claim 19 further comprising:

in response to determining that the key is present, extracting a decryption parameter from the key,

wherein the act of decrypting the encrypted portion of the graphics data is responsive to the decryption parameter.

22. The method of claim 19, further comprising, prior to the act of receiving the graphics data:

encrypting at least a portion of the graphics data; and

transmitting the graphics data.

23. The method of claim 22 wherein the act of transmitting the graphics data is performed using a system bus.

24. The method of claim 23 wherein the act of encrypting is performed by a central processing unit executing a graphics driver program.

25. The method of claim 22 wherein the act of transmitting the graphics data is performed using a network.

26. The method of claim 19 wherein the act of determining whether the key is present includes detecting a presence or absence of a key device.

27. The method of claim 19 wherein the act of determining whether the key is present includes detecting a presence or absence of key data.

28. The method of claim 19 wherein the act of decrypting the graphics data includes:

restoring the graphics data to its unencrypted state; and

perturbing a parameter value of the restored graphics data based on a perturbation parameter.

29. The method of claim 28 wherein the parameter value is a vertex coordinate of a primitive.

30. The method of claim 28 wherein the perturbation parameter is determined from the key.

31. The method of claim 30 wherein the perturbation parameter corresponds to a clearance level associated with the key.

32. A method for sharing encrypted graphics data among a plurality of users, the method comprising:

associating each of the plurality of users with a respective one of a plurality of keys for decrypting the encrypted graphics data;

receiving the encrypted graphics data at a recipient device;

receiving one of the plurality of keys at the recipient device, wherein the one of the plurality of keys is provided by the associated user; and

decrypting the encrypted graphics data based at least in part on the received key.

33. The method of claim 32 wherein each key includes an identifier of a clearance level and the act of decrypting the graphics data depends at least in part on the clearance level.

34. The method of claim 33 wherein during the act of decrypting, a perturbation is applied to the graphics data, the size of the perturbation being dependent on the clearance level.

35. The method of claim 33 wherein during the act of decrypting, the clearance level is used to determine whether to discard a portion of the graphics data.

36. The method of claim 32 wherein the act of associating each of the plurality of users with a respective one of the plurality of keys includes providing a respective hardware device for each user, each hardware device storing key data, and wherein the act of receiving one of the plurality of keys includes communicating with the hardware device.

37. The method of claim 36 wherein communicating with the hardware device includes receiving the hardware device in a receptacle of the recipient device.

38. The method of claim 32 wherein the act of associating each of the plurality of users with a respective one of the plurality of keys includes providing a password for each user, and wherein the act of receiving one of the plurality of keys includes receiving the password.